AMENDMENTS TO THE CLAIMS

In accordance with the PTO's amendment format, a detailed listing of all claims has been provided. A status identifier is provided for each claim in parentheses following each claim number. Changes to the claims are shown by strikethrough (for deleted text) or underlining (for added text).

In the Claims:

Claims 1, 4, 6, 22-26, 39, 42-44, 50, and 52-56 were previously pending.

Claims 1, 22, 39, 50, 54, and 56 are currently amended.

No new claims are added.

No claims are canceled in this response.

Claims 1, 4, 6, 22-26, 39, 42-44, 50, and 52-56 are pending.

Listing of Claims

1. (Currently amended) An assembly for physically transporting a user profile between network and standalone computing devices, for automatically logging onto one of the network or standalone computing devices, and for automatically configuring the logged-on network or standalone computing device with user-preferences and user-selected operating system characteristics according to the user profile, comprising:

a portable profile storage device having an interface to communicate with a physical key and having a secure memory to securely store the user profile; and

a removable passcode-activated physical key associated with the user that alternately enables access to the user profile in the memory when the physical key is passcode-activated and coupled with the interface and that disables access to the user profile when removed from the interface,

wherein the portable profile storage device makes the user profile accessible to a computing device if the portable profile storage device is coupled with the computing device, the physical key is coupled with the interface, and a user passcode activates the physical key; and

wherein the physical key first authenticates the user, then authenticates the portable profile storage device, then automatically logs the user onto the computing device, then automatically configures the computing device with the user-preferences and the user-selected operating system characteristics from the user profile.

2-3. (Canceled)

4. (Previously presented) An assembly as recited in claim 1, wherein the device securely stores a user's data to be made accessible when the user profile is made accessible.

5. (Canceled)

6. (Previously presented) An assembly as recited in claim 1, wherein the portable profile storage device stores a public encryption key and the physical key stores a corresponding private decryption key and access to the user profile in the secure memory is enabled upon verification that the public key and the private key are associated and the user passcode activates the physical key.

7-21. (Canceled)

22. (Currently amended) A computer system that stores user credentials, user-preferences, and user-selected operating system characteristics in a portable smart card secured memory assembly that automatically logs the user onto various network and standalone computing devices and automatically configures one of the logged on network or standalone computing devices with the user-preferences and user-selected operating system characteristics, comprising:

a computer having a portable ~~PCMCIA~~ device reader; and

a smart card secured memory assembly ~~physically sized in a form factor of a PCMCIA card~~ to compatibly interface with the portable ~~PCMCIA~~ device reader in the computer, the smart card secured memory assembly having data memory to store a user profile and a passcode-protected removable smart card that alternately enables access to the user profile when present and activated via the passcode and that disables access to the user profile when removed,

wherein the smart card first authenticates the user, then authenticates the user profile, then automatically logs the user onto the computer, then automatically configures the computer with the user-preferences and the user-selected operating system characteristics from the user profile.

23. (Original) A computer system as recited in claim 22, wherein the data memory comprises flash memory.

24. (Original) A computer system as recited in claim 22, wherein the smart card stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user data.

25. (Original) A computer system as recited in claim 22, wherein:

the smart card stores a first key;

the data memory stores a second key that is associated with the first key; and

the smart card is configured to authenticate the second key from the data memory using the first key as a condition for enabling access to the user data.

26. (Original) A computer system as recited in claim 22, wherein:

the smart card stores a passcode and a private key of a public/private key pair;

the data memory stores a public key of the public/private key pair; and

the smart card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key from the data memory using the private key as a condition for enabling access to the user data.

27-38. (Canceled)

39. (Currently amended) ~~An assembly, comprising:~~

The computer system as recited in claim 22, wherein the smart card secured memory assembly comprises a USB-compatible memory to store [[a]] the user profile ~~; and~~

~~a passcode-protected removable physical key to enable access to the user profile on the memory when the physical key communicatively interfaces with the memory~~ .

40-41. (Canceled)

42. (Previously presented) An assembly according to claim 39, wherein the memory stores a public key and the physical key stores a corresponding private key, and access to the user profile stored in the memory is enabled when the physical key is coupled with the memory, association of the public key and the private key is verified, and the correct passcode is entered.

43. (Previously Presented) An assembly according to claim 39, wherein the memory has a public area and a private area, wherein further the private area stores the data files.

44. (Previously Presented) An assembly according to claim 43, wherein the data files include a user profile and other data files.

45-49. (Canceled)

50. (Currently amended) A personal information carry on assembly for physically transporting a profile of a computing device user between a computing network and a standalone computing device, comprising:

removable means for storing data files;

an interface on the removable means for communicatively coupling and uncoupling with the computing network or the standalone computing device; and

detachable means for enabling passcode-protected access to data files on the removable means when the detachable means communicatively attaches to the removable means,

wherein the removable means includes a flash memory, and the data files include a user profile to configure the computing network and the standalone computing device, and

wherein the detachable means first authenticates the user, then authenticates the removable means, then automatically logs the user onto the computing device, then automatically configures the computing device with user-preferences and user-selected operating system characteristics from the user profile.

51. (Canceled)

52. (Previously Presented) An assembly according to claim 50, wherein the detachable means is to store a passcode, and access to the data files stored in the removable means is enabled upon authentication of a user-supplied passcode to a passcode stored on the detachable means.

53. (Previously Presented) An assembly according to claim 50, wherein the removable means stores a public key and the detachable means stores a corresponding private key, and access to the data files stored in the removable means is enabled upon verification that the public key and the private key are associated.

54. (Currently amended) A secure apparatus for physically transporting a profile of a computing device user between computing devices, comprising:

a first portable storage device, including:

a storage area for storing the profile and for storing a public key of an encryption key pair,

a first interface for communicatively coupling with one of the computing devices, and

a second interface;

a second portable storage device capable of coupling with the second interface, including:

a storage area for a private key of the encryption key pair, and

an authentication device for verifying a passcode from the user;

wherein the secure apparatus uploads the profile to a computing device in response to: the computing device being communicatively coupled with the secure apparatus, the private key complementing the public key, and the authentication device verifying the passcode received from the user, and

wherein the second portable storage device authenticates the user, then authenticates the first portable storage device, then automatically logs the user onto one of the computing devices, then automatically configures the logged on computing device with user-preferences and user-selected operating system characteristics from the profile.

55. (Previously presented) The secure apparatus as recited in claim 54, further comprising a driver included in one of the computing devices, to detect whether a removable device coupled with the computing device is the first portable storage device coupled with the second portable storage device.

56. (Currently amended) The secure apparatus as recited in claim 54, further comprising a logon module included in one of the computing devices to recognize that the secure apparatus is coupled with the computing device and the second portable storage device is coupled with the first portable storage device and to automatically log on the user.